



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/072,597	02/05/2002	Paul A. Cronic	2401P	1789

7590 01/23/2006

SAWYER LAW GROUP LLP
P.O. Box 51418
Palo Alto, CA 94303

EXAMINER

BAYAT, BRADLEY B

ART UNIT PAPER NUMBER

3621

DATE MAILED: 01/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/072,597	Applicant(s) CRONCE, PAUL A.	
	Examiner Bradley B. Bayat	Art Unit 3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03 November 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-26 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-26 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Status of Claims

This communication is in response to remarks and amendments filed on November 3, 2005.

- Claims 1, 11, 12, 15, 16, 23 and 24 have been amended.

Thus, claims 1-26 remain pending.

Response to Arguments

Applicant's arguments filed on November 3, 2005. have been fully considered but they are not persuasive.

Applicant has amended claims 1, 12 and 16 to recite that "at least one of the private or public keys" associated with the software product "is digitally signed by a publisher private key (response p. 10)." Claim 24 has been amended to recite that a publisher certificate is "digitally signed by" a certificate authority." Id. Dependent claims 1, 15 and 23 have been amended to recite "license request" instead of "license." Id. In paragraph 3 of the remarks, applicant incorrectly identifies the rejected claims as "1-30 and 34-35." Id. For clarity of the record, only claims 1-26 were pending and rejected in the previous action.

As per claims 1, 12 and 16, applicant argues that the cited reference (Venkatesan et al., 6,898,706 B1) "fails to teach or suggest such a software licensing mechanism and instead teaches a content protection scheme that protects non-executable data." Id. at 13. Thereafter, applicant repeats in its entirety column 5, lines 21-57 in the summary section of the cited reference. Applicant's background of the invention acknowledges that protection of content and licensing of content for authorized use have been a problem and represent one of the objects of applicant's

Art Unit: 3621

invention [0006-0011]. In fact, the cited reference highlights that such a distinction cannot be made in a DRM system, “since the DRM initiative holds significant promise as a mechanism that will sufficiently restrict illicit copying of Internet accessible software objects and hopefully, by doing so, assure a sufficient financial return to publishers of those objects for their legitimate consumer access and use (column 3, lines 59-67).

Applicant further argues that the cited reference fails to disclose a “chaining of certificates (response p. 14).” On the contrary, Venkatesan discloses, “[a]t run time, the key manager, in turn, checks integrity of all other critical components of enforcer 600 using digital signatures of their expected vendors. To achieve this, O/S 454 can utilize an authenticated boot process to assure its own security and then establish necessary chains of trust among various components of the O/S and particularly throughout enforcer 600 and DRM system 456 (column 19, lines 25-56).”

Applicant contends that the cited reference refers to a “secret key” yet the claimed invention provides for a private key (response p. 14). As is well known in the cryptographic art and disclosed in the background of the reference, “[d]epending on the specific cipher used, this secret can be, e.g., a simple key known only to a sender and a recipient, or can be a **private key** of a public/private key pair (column 3, lines 37-48; emphasis added).” The cited reference discloses that a “secret value” that may represent a public/private pair key would be associated with the software certificate (see columns 5-8; figure 5 and associated text). Furthermore, the reference discloses that the publisher could readily extract the fingerprint in that object. By querying its user database, the publisher could learn the identity of the client PC, in terms of its computer ID, that the pirate used, in some fashion, to commit piracy.

The publisher could then instruct the WA to revoke a software certificate that held by this particular client PC for use of that particular key. If the WA is also a certifying authority (CA), then a usual client certificate can simply be revoked. In this case, the watermark key itself does not need to be certified. For purposes of simplicity, we will assume throughout the remainder of the description, that these two authorities are the same (column 16, line 55-column 17, line 6). Moreover, the enforcer, as indicated in block 1350, decrypts the downloaded object, O.sub.fe.sup.WM, using the symmetric encryption key (k.sup.e.sub.i) extracted from the license to yield the decrypted, fingerprinted and watermarked object, M (i.e., O.sub.f.sup.WM), which is then stored within unencrypted buffer 650.

In addition, the verifier 620; in turn, compares the VID value contained in header 1010 and the PID value specified in the license (these VID and PID values being "expected" values) to actual VID and PID values extracted from the watermark detected in the object to determine if identical matches exist between the actual and expected values of the PID, and between the actual and expected values of the VID. Most importantly, the verifier also checks if the license is signed by the publisher whose PID value was found in the detected watermark. To accomplish this, the verifier requires the publisher's certificate, cert (PK.sub.VID). The encrypted store delivers this certificate together with the license. If issue and expiration times are used for both watermark keys and the license, verifier 620 will also determine whether the license was issued later than the watermark key and expires before the watermark key (i.e., "issue/expiration time conditions").

If these matches occur, the license is properly signed and, when applicable, the issue/expiration time conditions are met, verifier 620 passes, as symbolized by line 623, the

Art Unit: 3621

value of the rights vector V, also specified in the license, to the client O/S, as the protection state of this object, to control further access and use of object C.sub.i while that object resides in decrypted form (as object M) within unencrypted buffer 650. In particular, if the rights vector illustratively contains three separate one-bit values (v.sub.1, v.sub.2 and v.sub.3), as shown in FIG. 6, these bits, based on their current states, may specify use of the object as follows: v.sub.1 =allow/disallow running; v.sub.2 =allow/disallow permanent storage; and v.sub.3 =allow/disallow manipulation. Hence, bit v.sub.1 would be applied to control a state of software switch 654 situated at an output of buffer 650.

In the case of active objects, this switch, once set, would effectively permit the object to be executed or not, i.e., effectively pass through line 653, via switch 654, to output lead 655. In the case of passive objects, this switch would either permit a media driver, which will be used in rendering that object through a media card, to either render that object or not, again symbolized by effectively passing that object through line 653, via switch 654 to output lead 655. Bit v.sub.2 would be applied, as symbolized by line 607, to ES 610 to specify whether the encrypted object (C.sub.i) can remain within this store, or is to be purged from this store after the object, in decrypted form, has passed through unencrypted buffer 650 and has either been executed or rendered, as appropriate. In that regard, the value of the rights vector for a given object taken in conjunction with a current user request to access and/or use that object will, through object usage process 1400 (shown in FIG. 14).

As per claims 11, 15 and 23, applicant's arguments that the reference fails to disclose "preventing use of the software product on a different computer" is without merit (response p. 16)." The cited reference discloses a secure software license DRM system and method that can

Art Unit: 3621

be utilized via the Internet and remotely controlled through web servers and various computers (see Venkatesan front page 300). On the contrary, the copy protection scheme is not merely machine specific (response p. 16). Once a watermarked object is created, operation 850 (also shown in detail in FIG. 8 and discussed in the accompanying text below) is performed by the publisher to: produce a replica (copy) of the watermark object; impart a fingerprint, should it be used, into that object replica; and encrypt a resulting fingerprinted object for a requesting client PC, e.g., PC 400; and finally download a particular encrypted, fingerprinted and watermarked object to that client PC. Operation 850 is performed every time a client PC (or other computer) requests a download of a watermarked object (emphasis added).

Accordingly, the rejection is maintained and made **FINAL**.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-26 are rejected under 35 U.S.C. 102(e) as being anticipated by Venkatesan et al. (hereinafter Venkatesan), US Patent 6,898,706 B1.

As per the following claims, Venkatesan discloses:

1. A method for the delivery of secure software license information to authorize use of a software product, the method comprising the steps of:

(a) associating with a software publisher a private and public key pair, wherein the software publisher provides the software product and includes a software program and an

Art Unit: 3621

authorization program within the software product (fig 5, publisher 330 downloads file encrypted, including watermark keys and fingerprinted for client PC 520)

(b) associating a product private key and public key with the software product, wherein at least one of the product private and public keys is digitally signed by the publisher private key and including the product private and public keys with the authorization program (fig 5, upon payment by user, publisher issues and downloads to user electronic license with usage rights including secret key 550);

(c) upon invocation of the software product on a computer, (i) generating by the authorization program a license request containing user and product information, (ii) digitally signing the license request with the product private key, and (iii) transferring the signed license request to a key authority (figure 3, certificate authority 307A signs with private key becoming part of the secure container for transfer to the key authority in figure 4)

(d) in response to the key authority receiving the signed license request, (i) generating a license using data extracted from the license request and license terms, (ii) signing the license with the publisher private key, and (iii) transmitting the signed license to the authorizing program (figure 13A, license verification, object decryption and enforcement 1300); and

(e) validating the signed license using the publisher public key, and using the license terms to control the use of the software product (figure 13A, enforcer process 1320, fig 13B instruct access in accordance with usage conditions 1380).

2. The method of claim 1 further including the step of providing the publisher public key as a certificate (fig 12, publisher's public key certificate 1220).

3. The method of claim 2 further including the step of providing the product public key as a certificate (fig 11, license generation and download 1122 including PID and certified public key).

4. The method of claim 1 further including the step of providing the license in a data exchange format (fig 5, client PC and Publisher data exchange 545 and 555).

5. The method of claim 4 further including the step of using XML as the data exchange format (column 11, lines 1-23, note that XML encoding may occur within HTML content; XML DTD describes a subset of HTML 4.0 for embedded use within other XML).

6. The method of claim 1 further including the step of using the license returned from the key authority to deliver additional key information to the computer (fig 13A, enforcer process 1320).

7. The method of claim 1 wherein step (d) further includes the step validating the license request using digital certificates (fig 11, computer ID of client PC 1122).

8. The method of claim 1 wherein step (e) further included the step of validating the license response using digital certificates (fig 11, computer ID of client PC 1122).

9. The method of claim 1 wherein step (e) further included the step of validating the license

Art Unit: 3621

using the product information in the license, including product ID and publisher ID (figure 11, product Id and publisher 's symmetric encryption key 1122).

10. The method of claim 9 further including the step of transferring license terms to a separate security device for controlling the use of the software product (fig 5, encrypted store 610 includes license database 570 and object store 580).

11. The method of claim 1 wherein step (e) further included the step of preventing use of the software product on a different computer than that used to generate the license request by using a machine fingerprint embedded in the license request (fig 5, fingerprint for client PCj 520).

Claims 12-15 are directed to a method as recited above and are rejected as above.

16. A method for the delivery of secure software license information to authorize use of a software product, the method comprising the steps of:

a. associating with the software product to be authorized an authorization program and a set of certificates, including a publisher certificate and a product certificate, wherein each certificate contains a public key and is associated with a private key of a public/private key pair, wherein the product certificate is signed by the private key associated with the publisher certificate (figure 12 and associated text);

Art Unit: 3621

b. upon invocation of the software product on a computer, generating by the authorization program a formatted license request containing user and product information, signed using the private key associated with the product certificate (fig 11, client license request 1110);

c. transmitting the license request to a key authority in conjunction with a financial transaction (fig 11, request includes CID, client's public key, usage rights and payment information 1115);

d. generating by the key authority a formatted license that includes license terms, and user and product information extracted from the license request, wherein the license is signed with the publisher private key associated with the publisher certificate (fig 11, upon authorization of payment generating license 1122);

e. transmitting the signed license to the authorizing program (fig 11, transmit license to publisher's web server 1124); and

f. validating by the authorization program the license using the publisher and certificate authority certificates and the user and product information contained within the license document, whereby the validation using the publisher and certificate authority certificates establish a trusted link back to the certificate authority (fig 13 A license verification, object decryption and enforcement 1300, 1320) and;

g. using the license terms to control the use of the software product on the computer (fig 13B instruct use in accordance with rights and access 1380).

17. The method of claim 16 further including the step of formatting the license request and license documents using the proposed signed XML standard definition (column 11, lines 1-23,

Art Unit: 3621

note that XML encoding may occur within HTML content; XML DTD describes a subset of HTML 4.0 for embedded use within other XML).

18. The method of claim 16 further including the step of signing the product certificate using the publisher's private key, and signing the publisher certificate using the certificate authority's private key, thus establishing a trusted link from the product certificate back to the certificate authority (fig 15, 16 and associated text)

19. The method of claim 16 further including the step of signing the license request using the product private key, and including within the license request the product certificate (fig 11, step 1115).

20. The method of claim 16 further including the step of including financial transaction information within the license request (fig 11, step 1115)

21. The method of claim 20 further including the step of including financial transaction information within the license response (fig 11, step 1122).

22. The method of claim 16 wherein step (g) further includes the step of transferring the license terms to a separate security device for controlling the use of the software product (fig 11, step 1124 publisher's web server downloads license to EC 610).

Art Unit: 3621

23. The method of claim 16 wherein step (g) further includes the step of preventing use of the software product on a different computer than that used to generate the license request by using a machine fingerprint embedded in the license request (fig 5, fingerprint 520).

Claims 24-26 are directed to a method as recited above and are rejected as above.

Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

Art Unit: 3621

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- US Patent 6,611,812 B2 to Hurtado et al.
- US Patent 6,904,523 B2 to Bialick et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Bradley B. Bayat whose telephone number is 571-272-6704. The examiner can normally be reached on Tuesday - Friday 8 a.m.-6:30 p.m. and by email: bradley.bayat@uspto.gov. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached regarding urgent matters at 571-272-6712.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Art Unit: 3621

Any response to this action should be mailed to:


Commissioner of Patents and Trademarks
Washington, D.C. 20231

Or faxed to:

(571) 273-8300 - Official communications; including After Final responses.

(571) 273-6704 - Informal/Draft communications to the examiner.

bbb
January 13, 2006


Primary Examiner
AU 3621